UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,558	12/06/2001	Albert Young	3730.US.P	6325

56436 7590 11/28/2006

3COM CORPORATION
350 CAMPUS DRIVE
MARLBOROUGH, MA 01752-3064

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/016,558	YOUNG ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) *2-7, 20, 22-27, 40-42-47 & 60* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,8-19,21,28-39,41 and 48-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The RCE of 6/29/2006 and claims of 9/20/2006 were received and considered.

2. Claims 1-60 are pending.

3. Claims 2-7, 20, 22-27, 40, 42-47 & 60 are withdrawn from consideration.

4. Claims 1, 8-19, 21, 28-39, 41 & 48-59 are examined herein.

Specification

5. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: The specification does not disclose connecting a client to an access point via a wired connection.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 39 & 59 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

a. Regarding claims 39 & 59, it is unclear how the network access point and unauthenticated client device are coupled wired connection, when an access point is known in the art as a connector between a wireless device and a LAN. For the purposes of this Office Action, this claim is understood to mean that the two devices are coupled via a wireless connection, and is rejected accordingly. It is noted that, in this interpretation, the claims are identical to claims 38 & 58, respectively, and are therefore objected to accordingly. If applicant intends for "access point" to refer more broadly to any device to which the unauthenticated client device is connecting or any device through which the unauthenticated client device is passing information, than claims 21, 28-39, 41 & 48-59 are rejected under similar rationale as claims 1 & 8-19. However, it is believed that this broader interpretation is not supported by applicant's specification and therefore it is understood that an access point refers to a device connecting with a wireless client.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 18-19, 41 & 48-59 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

b. Regarding claims 18-19, the limitations "said first electronic device" and "said second electronic device" lacks sufficient antecedent basis. For the purposes of this Office Action, "said first electronic device" and "said second electronic device" are

understood to refer to said unauthenticated client device and said authentication server, respectively.

c. Regarding claim 41, the claim recites "In a computer-usable medium having computer-readable code embodied thereon, a computer-implemented method for authenticating ...". It is therefore unclear which statutory class the invention falls under. The above citation is understood to read "A computer-usable medium having computer-readable code embodied thereon that is executed by a computer to implement the method of: ..." such that the statutory class under which the claim falls is clearly a manufacture and discloses a functional interrelationship between the medium and the functional code on the medium.

d. Regarding claim 49, the claim recites that the network access point provides an interface between the client and server, however, claim 48 recites the limitation "said network access point is the central authentication server". *For the purposes of this action, this limitation is understood to read "wherein said network access point is communicatively coupled to the central authentication server".*

e. Regarding claim 49, it is unclear how the network access point can provide an interface between said authenticated client device and said central authentication server when the network access point is the central authentication server. The claims are rejected as best understood, such that the network access point is not the central authentication server.

f. Regarding claims 58-59, the claims recite "The computer implemented method", however, the independent claim is directed to a computer-usable medium. Therefore, these claims' preambles are understood to mean "The computer-usable medium".

10. All claims rejected above under 35 U.S.C. §112 are examined as best understood. Further, any claims dependent upon a claim rejected under 35 U.S.C. §112 are rejected at least based on this dependency.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 1 & 8-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over "PPP EAP TLS Authentication Protocol" by Aboba et al. (**Aboba**) in view of "Remote Authentication Dial In User Service (RADIUS)" by C. Rigney et al. (**Rigney**).

Regarding claim 1, Aboba discloses the EAP TLS protocol, comprising authenticating an authentication server (TLS authenticator) to an unauthenticated client device (TLS peer) communicatively coupled to the authentication server (TLS certificate, p. 9, step 7 & TLS certificate_verify message, p. 10, step 8), authenticating the unauthenticated client (TSL peer) to the authentication server (TLS authenticator) to produce an authenticated client device (TLS certificate, p. 9, step 8 & TLS finished message, p. 10, steps 8-9), generating a key (deriving new encryption keys, p. 7, §3.5) at the authenticated client device (TLS peer) and the authentication

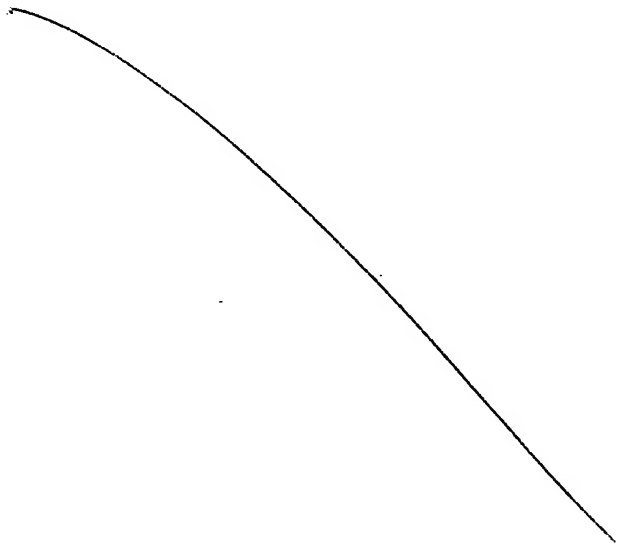
server (TSL authenticator/EAP server) (pp. 7-8, §3.5). Aboba lacks authenticating a user to a central authentication server using the authenticated client device (TLS peer). However, Rigney discloses authenticating a user (RADIUS request containing user's password, p. 5, §2) to a central authentication server (radius server) (p. 5, §2, ¶3) using PPP (p. 5, §2, ¶1) for the purpose of authenticating users and delivering services based on that authentication (p. 3, §1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba's EAP TLS protocol to authenticate a user to a RADIUS server using the key generated and using the authenticated client device. One of ordinary skill in the art would have been motivated to perform such a modification to authenticate the user securely and deliver services to the user, as taught by Rigney (p. 3, §1, ¶2 & p. 5, §2).

Regarding claim 8, Aboba discloses wherein said authentication server (TLS authenticator) is the central authentication server (RADIUS server, p. 2, §3.1, ¶2).

Regarding claim 9, Aboba discloses wherein a network device (authenticator) is employed for providing an interface (pass-through device, p. 2, §3.1, ¶2) between said unauthenticated client (TLS peer) and said central authentication server (RADIUS server, p. 2, §3.1, ¶2).

Regarding claim 10, Aboba discloses receiving a first standard message (containing PPP EAP-Response/Identity (MyID), p. 9, step 4) from said unauthenticated client device (TLS peer) at said network device (pass-through device, p. 2, §3.1, ¶2), forwarding said first standard message to said central authentication server (RADIUS server) from said network device (pass-through device, p. 2, §3.1, ¶2) and receiving said first standard message from said network device (pass-through device, p. 2, §3.1, ¶2) at said central authentication server (RADIUS server) whereby said unauthenticated client device is identified (p. 9, step 4) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2).

Regarding claim 11, Aboba discloses sending a second standard message (containing TLS certificate, p. 9, step 7) to said network device (pass-through device, p. 2, §3.1, ¶2) from said central authentication server (RADIUS server, p. 2, §3.1, ¶2) and forwarding (p. 2, §3.1, ¶2) said second standard message (TLS certificate, p. 9, step 7) to said unauthenticated client device (TLS peer, pl. 7) from said network device (pass-through device, p. 2, §3.1, ¶2), whereby said central authentication server (RADIUS server) is authenticated to said unauthenticated client (TLS peer) device (TSL certificate_verify, p. 10, step 8).



Regarding claim 12, Aboba discloses sending a third standard message (containing TLS certificate, p. 9, step 8) to said network device (pass-through device, p. 2, §3.1, ¶2) from said unauthenticated client (TLS peer) device and forwarding (p. 2, §3.1, ¶2) said third standard message (TLS certificate, p. 9, step 8) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) from said network device (pass-through device, p. 2, §3.1, ¶2), whereby said unauthenticated client (TLS peer) device is authenticated to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) as the authenticated client device (TLS change_cipher_spec indicates that authentication is successful and further information will be encrypted, p. 10, step 9).

Regarding claim 13, Aboba discloses that the first standard message comprises a standard EAP-TLS message (p. 9, step 4).

Regarding claim 14, Aboba discloses wherein the second standard message (p. 9, step 7) comprises a key exchange (TLS server_key_exchange, p. 9, step 7) from said central authentication server (RADIUS server/authenticator) to said client device (TLS peer) (p. 9, step 7).

Regarding claim 15, Aboba discloses wherein said second standard message comprises a standard EAP-TLS protocol message (p. 9, step 7).

Regarding claim 16, Aboba discloses wherein said third standard message (p. 9, step 8) comprises a key exchange (TLS client_key_exchange, p. 9, step 8) from said client device (TLS peer) to said central authentication server (RADIUS server/authenticator, p. 9, step 8).

Regarding claim 17, Aboba discloses wherein said third standard message comprises a standard EAP-TLS protocol message (p. 9, step 8).

13. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Aboba** and **Rigney**, as applied to claim 1 above, in further view of **one having ordinary skill** at the time the invention was made.

Regarding claim 18, Aboba lacks explicitly the type of connection between the devices claimed. However, wired connections are well known to be less expensive and faster. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba to employ a wired connection between the devices. One of ordinary skill in the art would have been motivated to perform such a modification to increase the speed and decrease the cost of the system. This is well known in the art.

14. Claims 19, 21, 28-39, 41 & 48-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Aboba** and **Rigney**, as applied at least to claim 1 above, in further view of How Networks Work by Derfler et al. (**Derfler**).

Regarding claim 19, Aboba lacks the first and second devices being communicatively coupled by a wireless connection. However, Derfler teaches that wireless LANs allow users to move around without losing their connection (p. 114). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba to make use of a wireless LAN to couple the client, server and network access point (proxy) (such that the network access point is a wireless access point). One of ordinary skill in the art would have been motivated to perform such a modification to enable users to move around without losing their connection, as taught by Derfler (p. 114).

Regarding claim 21, Aboba discloses a central authentication server (TLS authenticator/EAP server, pp. 7-8, §3.5), an unauthenticated client device (TLS peer) (p. 2, §3.1) coupled to said network and also discloses the EAP TLS protocol, comprising authenticating an authentication server (TLS authenticator) to an unauthenticated client device (TLS peer) communicatively coupled to the authentication server (TLS certificate, p. 9, step 7 & TLS certificate_verify message, p. 10, step 8), authenticating the unauthenticated client (TSL peer) to the authentication server (TLS authenticator) to produce an authenticated client device (TLS certificate, p. 9, step 8 & TLS finished message, p. 10, steps 8-9), generating a key (deriving new encryption keys, p. 7, §3.5) at the authenticated client device (TLS peer) and the authentication server (TSL authenticator/EAP server) (pp. 7-8, §3.5). Aboba lacks authenticating a user to a central authentication server using the authenticated client device (TLS peer) to send or receive information over the computer system network. However, Rigney discloses authenticating a user (RADIUS request containing user's password, p. 5, §2) to a central authentication server (radius server) (p. 5, §2, ¶3) using PPP (p. 5, §2, ¶1) for the purpose of authenticating users and delivering services based on that authentication (p. 3, §1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba's EAP TLS protocol to authenticate a user to a RADIUS server using the key generated and using the authenticated client device and to send or receive information over the network (render services). One of ordinary skill in the art would have been motivated to perform such a modification to authenticate the user securely and deliver services to the user, as taught by Rigney (p. 3, §1, ¶2 & p. 5, §2). Aboba, as modified above, lacks the authentication server mentioned above (Aboba's pass-through authentication device, see Aboba, p. 2, §3.1, ¶2) being a

network access point. However, Derfler teaches that in wireless network, mobile computers (peers) (p. 114) are connected to existing LANs, the Internet, etc. through access points (p. 114). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba to have the server act as an access point. One of ordinary skill in the art would have been motivated to perform such a modification to enable mobile peers to communicate with the existing Ethernet, the Internet, etc. (also Aboba's back end server, see Aboba, p. 2, §3.1, ¶2).

Regarding claim 28, as modified above, Aboba discloses wherein said network access point is a wireless access point (Derfler, pp. 114-115).

Regarding claim 29, as modified above, Aboba discloses wherein the network access point is an interface between said authenticated client device (TLS peer) and said central authentication server (Derfler, pp. 114-115).

Regarding claim 30, Aboba discloses receiving a first standard message (containing PPP EAP-Response/Identity (MyID), p. 9, step 4) from said unauthenticated client device (TLS peer) at said access point (pass-through device, p. 2, §3.1, ¶2), forwarding said first standard message to said central authentication server (RADIUS server) from said access point (pass-through device, p. 2, §3.1, ¶2) and receiving said first standard message from said access point (pass-through device, p. 2, §3.1, ¶2) at said central authentication server (RADIUS server) whereby said unauthenticated client device is identified (p. 9, step 4) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2).

Regarding claim 31, Aboba discloses sending a second standard message (containing TLS certificate, p. 9, step 7) to said access point (pass-through device, p. 2, §3.1, ¶2) from said central authentication server (RADIUS server, p. 2, §3.1, ¶2) and forwarding (p. 2, §3.1, ¶2) said second standard message (TLS certificate, p. 9, step 7) to said unauthenticated client device (TLS peer, pl. 7) from said access point (pass-through device, p. 2, §3.1, ¶2), whereby said central authentication server (RADIUS server) is authenticated to said unauthenticated client (TLS peer) device (TSL certificate_verify, p. 10, step 8).

Regarding claim 32, Aboba discloses sending a third standard message (containing TLS certificate, p. 9, step 8) to said access point (pass-through device, p. 2, §3.1, ¶2) from said unauthenticated client (TLS peer) device and forwarding (p. 2, §3.1, ¶2) said third standard message (TLS certificate, p. 9, step 8) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) from said access point (pass-through device, p. 2, §3.1, ¶2), whereby said unauthenticated client (TLS peer) device is authenticated to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) as the authenticated client device (TLS change_cipher_spec indicates that authentication is successful and further information will be encrypted, p. 10, step 9).

Regarding claim 33, Aboba discloses that the first standard message comprises a standard EAP-TLS message (p. 9, step 4).

Regarding claim 34, Aboba discloses wherein the second standard message (p. 9, step 7) comprises a key exchange (TLS server_key_exchange, p. 9, step 7) from said central authentication server (RADIUS server/authenticator) to said client device (TLS peer) (p. 9, step 7).

Regarding claim 35, Aboba discloses wherein said second standard message comprises a standard EAP-TLS protocol message (p. 9, step 7).

Regarding claim 36, Aboba discloses wherein said third standard message (p. 9, step 8) comprises a key exchange (TLS client_key_exchange, p. 9, step 8) from said client device (TLS peer) to said central authentication server (RADIUS server/authenticator, p. 9, step 8).

Regarding claim 37, Aboba discloses wherein said third standard message comprises a standard EAP-TLS protocol message (p. 9, step 8).

Regarding claims 38-39, Aboba, as modified above, discloses wherein said unauthenticated client device and said network access point are communicatively coupled by a wireless connection (Derfler, pp. 114-115).

Regarding claim 41, Aboba discloses in a computer-usable medium (Aboba's disclosure deals with computers) a method comprising authenticating an authentication server (TLS authenticator) to an unauthenticated client device (TLS peer) communicatively coupled to the authentication server (TLS certificate, p. 9, step 7 & TLS certificate_verify message, p. 10, step 8), authenticating the unauthenticated client (TSL peer) to the authentication server (TLS authenticator) to produce an authenticated client device (TLS certificate, p. 9, step 8 & TLS finished message, p. 10, steps 8-9), generating a key (deriving new encryption keys, p. 7, §3.5) at the authenticated client device (TLS peer) and the authentication server (TSL authenticator/EAP server) (pp. 7-8, §3.5). Aboba lacks authenticating a user to a central authentication server using the authenticated client device (TLS peer) to send or receive information over the computer system network. However, Rigney discloses authenticating a user (RADIUS request containing user's password, p. 5, §2) to a central authentication server (radius server) (p. 5, §2, ¶3) using

PPP (p. 5, §2, ¶1) for the purpose of authenticating users and delivering services based on that authentication (p. 3, §1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba's EAP TLS protocol to authenticate a user to a RADIUS server using the key generated and using the authenticated client device and to send or receive information over the network (render services). One of ordinary skill in the art would have been motivated to perform such a modification to authenticate the user securely and deliver services to the user, as taught by Rigney (p. 3, §1, ¶2 & p. 5, §2). Aboba, as modified above, lacks the authentication server mentioned above (Aboba's pass-through authentication device, see Aboba, p. 2, §3.1, ¶2) being a network access point. However, Derfler teaches that in wireless network, mobile computers (peers) (p. 114) are connected to existing LANs, the Internet, etc. through access points (p. 114). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Aboba to have the server act as an access point. One of ordinary skill in the art would have been motivated to perform such a modification to enable mobile peers to communicate with the existing Ethernet, the Internet, etc. (also Aboba's back end server, see Aboba, p. 2, §3.1, ¶2).

Regarding claim 48, as modified above, Aboba discloses wherein said network access point is communicatively coupled to the central authentication server (Derfler, pp. 114-115).

Regarding claim 49, as modified above, Aboba discloses wherein the network access point is an interface between said authenticated client device (TLS peer) and said central authentication server (Derfler, pp. 114-115).

Regarding claim 50, Aboba discloses receiving a first standard message (containing PPP EAP-Response/Identity (MyID), p. 9, step 4) from said unauthenticated client device (TLS peer) at said access point (pass-through device, p. 2, §3.1, ¶2), forwarding said first standard message to said central authentication server (RADIUS server) from said access point (pass-through device, p. 2, §3.1, ¶2) and receiving said first standard message from said access point (pass-through device, p. 2, §3.1, ¶2) at said central authentication server (RADIUS server) whereby said unauthenticated client device is identified (p. 9, step 4) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2).

Regarding claim 51, Aboba discloses sending a second standard message (containing TLS certificate, p. 9, step 7) to said access point (pass-through device, p. 2, §3.1, ¶2) from said central authentication server (RADIUS server, p. 2, §3.1, ¶2) and forwarding (p. 2, §3.1, ¶2) said second standard message (TLS certificate, p. 9, step 7) to said unauthenticated client device (TLS peer, pl. 7) from said access point (pass-through device, p. 2, §3.1, ¶2), whereby said central authentication server (RADIUS server) is authenticated to said unauthenticated client (TLS peer) device (TSL certificate_verify, p. 10, step 8).

Regarding claim 52, Aboba discloses sending a third standard message (containing TLS certificate, p. 9, step 8) to said access point (pass-through device, p. 2, §3.1, ¶2) from said unauthenticated client (TLS peer) device and forwarding (p. 2, §3.1, ¶2) said third standard message (TLS certificate, p. 9, step 8) to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) from said access point (pass-through device, p. 2, §3.1, ¶2), whereby said unauthenticated client (TLS peer) device is authenticated to said central authentication server (RADIUS server, p. 2, §3.1, ¶2) as the authenticated client device (TLS change_cipher_spec indicates that authentication is successful and further information will be encrypted, p. 10, step 9).

Regarding claim 53, Aboba discloses that the first standard message comprises a standard EAP-TLS message (p. 9, step 4).

Regarding claim 54, Aboba discloses wherein the second standard message (p. 9, step 7) comprises a key exchange (TLS server_key_exchange, p. 9, step 7) from said central authentication server (RADIUS server/authenticator) to said client device (TLS peer) (p. 9, step 7).

Regarding claim 55, Aboba discloses wherein said second standard message comprises a standard EAP-TLS protocol message (p. 9, step 7).

Regarding claim 56, Aboba discloses wherein said third standard message (p. 9, step 8) comprises a key exchange (TLS client_key_exchange, p. 9, step 8) from said client device (TLS peer) to said central authentication server (RADIUS server/authenticator, p. 9, step 8).

Regarding claim 57, Aboba discloses wherein said third standard message comprises a standard EAP-TLS protocol message (p. 9, step 8).

Regarding claims 58-59, Aboba, as modified above, discloses wherein said unauthenticated client device and said network access point are communicatively coupled by a wireless connection (Derfler, pp. 114-115).

Conclusion

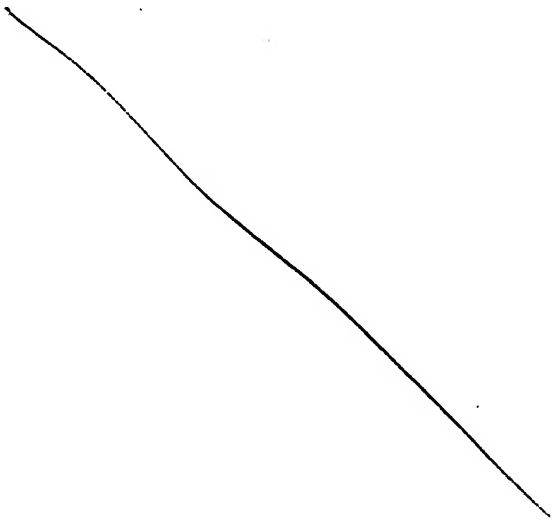
15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

g. The Stallings reference is cited for teaching SSL.

h. The Haverinen, Rahman and Kokudo references are cited for teaching wireless authentication.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

November 20, 2006